



**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

Aktenzeichen: 199 11 221.5
Anmeldetag: 12. März 1999
Anmelder/Inhaber: DeTeMobil Deutsche Telekom MobilNet GmbH,
Bonn/DE
Bezeichnung: Verfahren zur Verteilung von Schlüsseln an Teil-
nehmer von Kommunikationsnetzen
IPC: H 04 L, H 04 M, H 04 Q

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ur-
sprünglichen Unterlagen dieser Patentanmeldung.

München, den 04. Oktober 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiebinger

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn

Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, nach dem Oberbegriff des unabhängigen Patentanspruchs. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts z.B. gegenüber einem Mehrwertdiensteknoten des Kommunikationsnetzes authentisieren.

Heute authentisiert sich ein Teilnehmer von Telekommunikationsdiensten beim Zugang zu Mehrwertdiensteknoten wie z. B. einer Mobilbox, durch Eingabe eines Paßworts und Nutzernamens. In GSM-Mobilfunknetzen wird dabei meist durch die Signalisierung die Mobilteilnehmer-Rufnummer (MSISDN) als Nutzername übertragen, womit eine explizite Angabe durch den Nutzer entfällt.

Die Vergabe und Nutzung des Paßworts (hier gleichbedeutend mit Schlüssel) ist ein kritischer Vorgang, da durch unerwünschte Offenlegung oder bewußtes Ausspähen dem Nutzer erheblicher Schaden durch Mißbrauch zugefügt werden kann. Neue Paßwörter werden daher häufig per Einschreibebrief versandt, was organisatorisch und technisch einen erheblichen Aufwand bedeutet und zugleich einen Zeitverzug, bis ein Paßwort beim Nutzer eintrifft.

Geschieht darüber hinaus der Zugang zum Mehrwertdiensteknoten über unsichere Netze wie z. B. das Internet, besteht die Gefahr, daß Nutzername und Paßwort unberechtigterweise abgehört und mißbraucht werden.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäss wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdiensteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Der berechtigte Nutzer der (U)SIM kann die Möglichkeit nutzen, den Schlüssel in andere Endgeräte zu transferieren bzw. mit dem mobilen oder anderen Endgeräten über Internet, PSTN oder ISDN auf die Mehrwertdiensteknoten zuzugreifen. Das Authentikationsverfahren zwischen Endgerät und Mehrwertdiensteknoten sowie der Transfer eines Schlüssels vom mobilen Endgerät auf ein anderes kann mit bestehenden Algorithmen gelöst werden und ist nicht Gegenstand der Erfindung.

In einer ersten Ausführungsvariante der Erfindung ist vorgesehen, dass der Nutzer einen neuen Schlüssel bei Bedarf durch eine Kurznachricht (SMS) abrufen. Dazu sendet er eine Kurznachricht mit bestimmten Inhalt an eine durch den Netzbetreiber vorgegebene Zieladresse, die einer Sicherheitseinrichtung zugeordnet ist. Als Antwort erhält er von dieser Adresse ein Paßwort im Klartext zurück. Mit diesem Paßwort kann sich der Nutzer nun gegenüber einem Mehrwertdiensteknoten authentisieren.

In einer zweiten Ausführungsvariante der Erfindung, die ein höheres Sicherheitsniveau aufweist, ist vorgesehen, dass durch die Verwendung eines Programms auf der (U)SIM (Kartenapplikation), welches als Client mit dem Mobilfunknetz kommuniziert, alle Kommunikationsvorgänge zwischen Mobilstation und Sicherheitseinrichtung mit einem Ende-zu-Ende Verschlüsselungsverfahren verschlüsselt werden. In vorteilhafter Weise kann das Programm dem Nutzer eine menügeführte Oberfläche auf dem mobilen Endgerät bieten, mit der Schlüssel abgerufen und verwaltet werden können.

Zur Anforderung eines Schlüssels wählt der Nutzer z.B. einen entsprechenden Menüpunkt auf seinem Endgerät. Das Mobilfunknetz antwortet mit einer verschlüsselten Nachricht, die direkt an die Kartenapplikation gerichtet ist. Die Kartenapplikation speichert den Schlüssel in einem geschützten Speicherbereich der (U)SIM ab.

Zur Authentisierung gegenüber einem Mehrwertdiensteknoten wählt der Nutzer nach Eingabe einer PIN z.B. einen entsprechenden Menüpunkt an. Je nach Authentisierungsalgorithmus ist vorgesehen, dass

- der Schlüssel entweder im Klartext angezeigt und kann vom Nutzer weiterverwendet werden kann;
- der Schlüssel direkt zum Mehrwertdiensteknoten übertragen wird;
- der Schlüssel zu einem anderen Endgerät transferiert und dort weiterverwendet werden kann.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Im folgenden wird die Erfindung anhand eines Beispiels unter Bezugnahme auf eine Zeichnungsfigur näher beschrieben. Aus dem Beispiel, der Zeichnung und ihrer Beschreibung gehen weitere Merkmale und Vorteile der Erfindung hervor

Figur 1 zeigt eine Darstellung der beteiligten Systeme zur Durchführung des Verfahrens.

Die Mobilstation 3, welche ein Endgerät 4 umfasst, beherbergt in bekannter Weise die (U)SIM 5, auf der die Schlüssel zur Nutzerauthentikation gespeichert werden. Die Sicherheitseinrichtung umfasst einen Sicherheits-Server 9, der die Schlüssel nach einem vom Betreiber gewählten Algorithmus erzeugt, in einer Datenbank 10 speichert und die Schlüssel auf Anforderung 1 eines Teilnehmers an die (U)SIM 5 und die vom Teilnehmer nutzbaren Mehrwertdiensteknoten 11 verteilt.

Das Short Message Service Center 8 des Mobilfunknetzes 7 übermittelt die Schlüssel in Form von Kurznachrichten (SM) 2 zwischen Sicherheits-Server 9 und Mobilstation 3. Dies ist hier nur beispielhaft angegeben. Als Übermittlungseinrichtungen können z. B. auch GPRS-Knoten verwendet werden.

Gemäss einer ersten beim erfindungsgemässen Verfahren angewandten Sicherheitsstufe fordert der Teilnehmer einen Schlüssel über seine Mobilstation 3 durch eine Kurznachricht 1 an.

Der Sicherheits-Server 9 wertet die Anforderung aus, indem die Absendeadresse (MSISDN) des Teilnehmers auf Berechtigung geprüft wird, und sendet den oder die Schlüssel in einer Kurznachricht 2 an die Mobilstation 3, wo sie auf der (U)SIM 5 gespeichert wird. Darüber hinaus sendet der Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11. Die Schlüsselverteilung ist damit beendet. Der Nutzer kann sich nun je nach gewähltem Endgerät 4 und Zugangsweg (Mobilfunk, ISDN, Internet, etc.) gegenüber dem Mehrwertdiensteknoten 11 authentisieren.

Bei dieser niedrigen ersten Sicherheitsstufe basiert die Sicherheit der Schlüsselverteilung auf der Abhörsicherheit des GSM-/UMTS-Netzes und der Nutzeridentifikation per MSISDN. Einmal auf der (U)SIM gespeichert sind die Schlüssel über die Standard-PIN geschützt.

Bei der zweiten, erhöhten Sicherheitsstufe kann das SIM Application Toolkit (SAT) nach GSM 11.14 eingesetzt werden. Dazu wird eine SAT-Applikation auf die (U)SIM 5 eingebracht, die in dieser Client-Server-Konfiguration mit dem Sicherheits-Server 9 über das GSM- oder UMTS-Netz 7 kommuniziert.

Der Nutzer fordert Schlüssel über sein Endgerät 4 menüunterstützt über die SAT-Applikation an. Dazu muß er sich gegenüber der (U)SIM 5 mit einer zweiten PIN identifizieren, die er z.B. über die Tastatur des Endgeräts 4 eingibt. Danach versendet die SAT-Applikation eine verschlüsselte Anforderung 1 an den Sicherheits-Server 9, der die Anforderung verarbeitet. Der Sicherheits-Server 9 prüft die verschlüsselte Anforderung auf Echtheit anhand der Verschlüsselung sowie der Absendeadresse (MSISDN).

Bei positiv ausgefallener Prüfung erzeugt der Sicherheits-Server 9 den oder die Schlüssel für den Nutzer und sendet sie an die SAT-Applikation der (U)SIM 5 zurück. Die SAT-Applikation nimmt die Schlüssel entgegen und speichert sie in einem besonders geschützten Bereich der (U)SIM 5 ab. Darüber hinaus sendet der

Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11.

Der Zugriff auf die Schlüssel ist wiederum menügesteuert nach Eingabe einer PIN über die Kartenapplikation möglich, die einen ungebrauchten Schlüssel auf dem Display des Endgeräts 4 anzeigt oder auf Wunsch in einem ungeschützten SIM-Kartenspeicherbereich ablegt. Von dort kann dieser Schlüssel in einen PC/Laptop mittels Standard-Zugriffssoftware ausgelesen werden, z. B. mittels Chipkartenleser oder Infrarot-Schnittstelle des GSM-/UMTS-Endgeräts.

Alternativ und je nach Sicherheitsanforderung kann der Schlüssel auch vor dem Nutzer verborgen bleiben und vertraulich zwischen (U)SIM 5 und Mehrwertdiensteknoten 11 bzw. von der (U)SIM 5 zum Laptop/PC zwecks späterer Verwendung übertragen werden.

Ein besonderes Kennzeichen der zweiten Sicherheitsstufe ist eine zusätzliche Verschlüsselung der ausgetauschten Kurznachrichten 1, 2 zwischen dem Sicherheits-Server 9 (Server-SW) und der Software auf der (U)SIM 5 (Client-SW). Dadurch ist eine Ende-zu-Ende-Sicherheit zwischen Server-SW und Client-SW gegeben. Der Nutzer hat dabei vorzugsweise keine Kenntnis der dazu notwendigen Schlüssel. Als Verschlüsselungsalgorithmen zwischen Client und Server können Standardverfahren wie z. B. Triple-DES oder RSA zum Einsatz kommen.

Die für die Zusatzverschlüsselung notwendigen Schlüssel werden einmalig bei Personalisierung der (U)SIM eingebracht sowie auf den Sicherheits-Server geladen.

Zeichnungslegende

- 1 **Signalfluss: Schlüssel anfordern**
- 2 **Signalfluss: Schlüssel laden**
- 3 **Mobilstation**
- 4 **Endgerät**
- 5 **(U)SIM**
- 6 **Luftschnittstelle**
- 7 **Mobilfunknetz**
- 8 **Kurznachrichtendienst-Zentrale**
- 9 **Sicherheitseinrichtung (Server)**
- 10 **Datenbank**
- 11 **Mehrwertdiensteknoten**

Patentansprüche

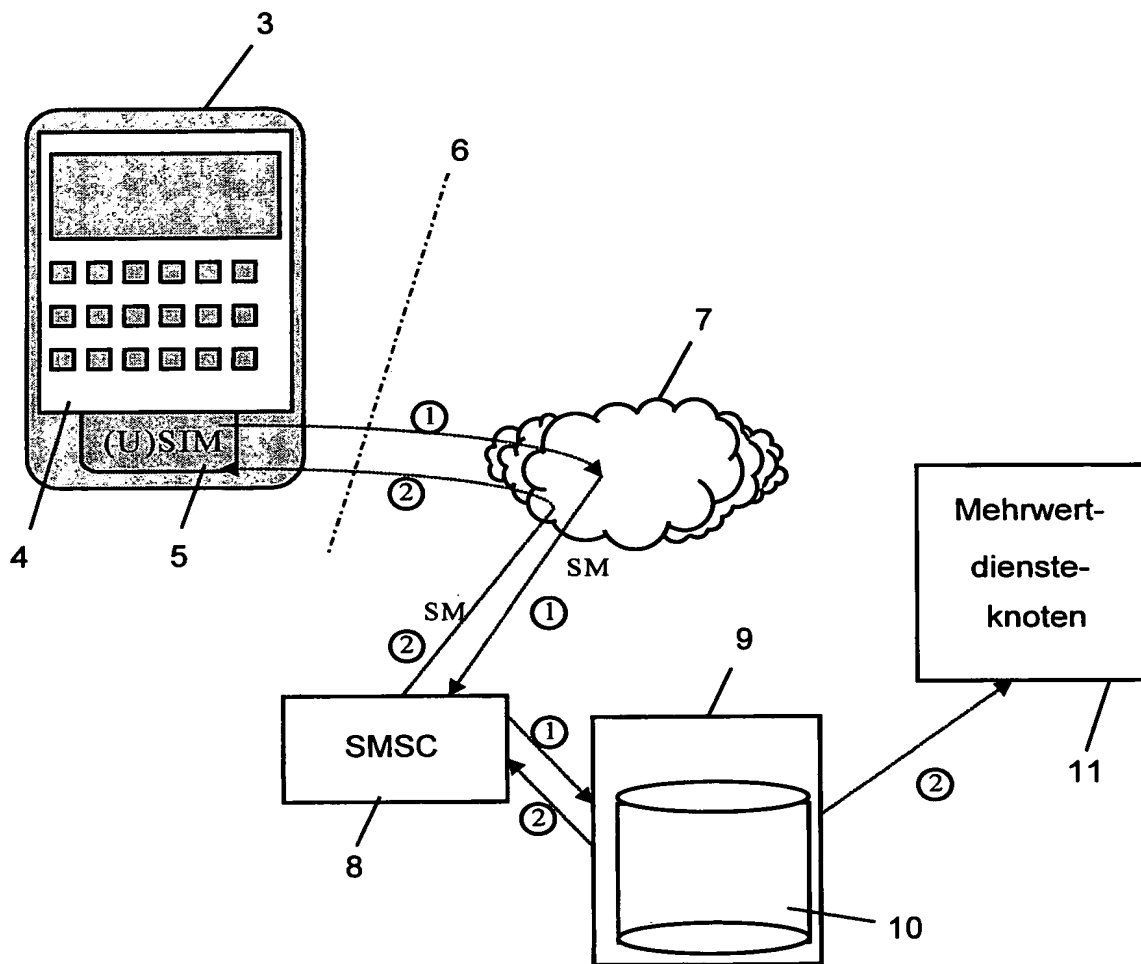
1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, dadurch gekennzeichnet,
dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und
dass auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation/ Endgerät des Teilnehmers übertragen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,
dass auf der SIM der Mobilstation eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung der zwischen Mobilstation und Sicherheitseinrichtung übertragenen Informationen vornimmt.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet,
dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber der (U)SIM durch Eingabe einer PIN identifizieren muss.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet,
dass der übertragene Schlüssel im Endgerät und/oder dem Teilnehmeridentitätsmodul U(SIM) der Mobilstation abgespeichert wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet,
dass der übertragene Schlüssel auf einem geschützten Speicherbereich der U(SIM) abgespeichert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes erfolgt.
7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes in Form einer Kurznachricht (SM) erfolgt.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass bei Anforderung des Schlüssels die Berechtigung des Teilnehmers durch Auswertung der Mobilteilnehmer-Rufnummer MSISDN geprüft wird.
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Sicherheitseinrichtung den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten sendet.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen. Diese Schlüssel werden z.B. für den Zugang zu Mehrwertdiensten benötigt. Hierbei besteht das Problem, die Schlüssel sicher und vor allem unkompliziert an die Teilnehmer zu verteilen.

Erfindungsgemäss wird dies dadurch erreicht, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.



FIGUR 1